REMARKS

Claims 1-30 are pending in this application, with claims 1, 12, 21 and 29 being independent. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 21-22 and 24-28 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Trostle (U.S. 5,919,257). Claims 1-20, 23 and 29-30 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Trostle and in further view of Gluck (U.S. 5,948,104). These contentions are respectfully traversed.

Independent claim 21 recites, "a network; a security operation center coupled with the network; and one or more machines coupled with the network, each machine comprising a communication interface and a memory including an execution area configured to perform operations comprising examining a set of instructions embodying an invoked application to identify the invoked application, obtaining application-specific intrusion criteria, and monitoring network communications for the invoked application using the application-specific intrusion criteria to detect an intrusion." (Emphasis added.)

Trostle describes examining executable programs during pre-boot of a workstation to determine if any illicit changes have

been made to the selected executable programs; and if changes are detected, the user and/or administrator is notified. (*See* Trostle at col. 1, line 66 to col. 3, line 3.) The executable programs of Trostle are deliberately examined during pre-boot, which is before the applications are invoked. In contrast, the subject matter of claim 21 covers examining a set of instructions embodying an application that has been invoked (i.e., has been activated and is running). (*See e.g.*, Specification at ¶s 19-20 and 29.) This is the exact opposite of Trostle, where the objective is to detect illicit changes before the workstation boots up, i.e., before any applications on the workstation are invoked.

The Office now asserts that, "The claimed invention broadly claims monitoring invoked applications and not to what applicant believes it as limiting to when or how the intrusion detection programs are invoked." (*See* OA mailed 07/17/2006 at p. 16, lines 13-15.) First, it should be noted that when or how intrusion detection programs are invoked is not the issue, since it is the application to be monitored that is at issue. Second, claim 21 clearly recites examining a set of instructions embodying an invoked application to identify the invoked application. Thus, the examining is performed on an application that has been invoked. The Office has failed to explain how

Trostle's pre-boot detection of prior illicit changes to executable programs (which by definition occurs before any of those executable programs are invoked) can be considered examining a set of instructions embodying an invoked application to identify the invoked application.

Moreover, the background of Trostle clearly teaches away from modifying Trostle to examine already invoked applications:

> Intrusion detection programs (i.e., virus checking programs) are commonly used in order to detect unauthorized modifications to executable programs. However, a particular problem with these intrusion detection programs is that they operate only after the operating system has been started. Therefore, the intrusion detection program is untrusted, and can be altered by a hacker since it operates after the operating system has initiated operation. [...] Therefore, the integrity of a[n] intrusion detection program which operates following system boot is suspect due to its vulnerability to attack, by for example, a Trojan horse.

(*See* Trostle at col. 1, lines 39-54.) This portion of Trostle clearly indicates that Trostle considers intrusion detection programs that operate only after the operating system has been started to be problematic. Thus, Trostle teaches away from examining a set of instructions embodying an invoked application.

Furthermore, even if Trostle could be modified to examine the executable programs after they are invoked, this would not result in the presently claimed subject matter. Independent claim 21 recites, "obtaining application-specific intrusion criteria, and monitoring network communications for the invoked application using the application-specific intrusion criteria to detect an intrusion." The Office now equates the trusted hash value for an executable program in Trostle with the claimed application-specific intrusion criteria. (*See* OA mailed 07/17/2006 at p. 3, lines 12-19.) However, even assuming this claim construction is appropriate (which is not conceded), Trostle still does not describe monitoring network communications as claimed.

Trostle describes examining executable programs during pre-boot of a workstation to determine if any illicit changes have been made to the selected executable programs; and if changes are detected, the user and/or administrator is notified. (*See* Trostle at col. 1, line 66 to col. 3, line 3.) Trostle also describes the use of signed pre-boot modules to enhance security between workstation and server, and a signature "used for background authentication and to further assist in validating the authenticity of packets transmitted by the workstation onto the network." (*See* Trostle at col. 5, lines 28-42; and col. 6,

lines 13-17.) However, while Trostle's prevention of unauthorized replacement or modification of the downloaded modules is considered by the Office to be a form of intrusion prevention (*see* OA mailed 07/17/2006 at page 16, line 22 to page 17, line 4), Trostle does not indicate that a trusted hash value is used to monitor network communications in the course of Trostle's prevention of unauthorized replacement or modification of the downloaded modules.

Thus, Trostle does not describe obtaining application-specific intrusion criteria, and monitoring network communications for the invoked application using the application-specific intrusion criteria to detect an intrusion, as recited in claim 21 (even under the claim construction currently adopted by the Office). For all of the above reasons, independent claim 21 should be in condition for allowance. Dependent claims 22-28 should be patentable based on the above arguments and the additional recitations they contain.

Independent claim 1 recites, "examining a set of instructions embodying an invoked application to identify the invoked application; obtaining an application-specific intrusion detection signature; and monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion." (Emphasis added.)

Gluck fails to cure the defects of Trostle discussed above. Thus, for at least the reasons discussed above in connection with claim 21, independent claim 1 should be in condition for allowance.

Independent claim 12 recites, "examining a set of instructions embodying an invoked application to identify the invoked application; obtaining an application-specific intrusion detection signature; and monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion" (Emphasis added.) Gluck fails to cure the defects of Trostle discussed above. Thus, for at least the reasons discussed above in connection with claim 21, independent claim 12 should be in condition for allowance.

Independent claim 29 recites, "a security operation center; one or more machines, each machine including means for identifying a process, obtaining a process-specific intrusion detection signature, and monitoring network communications for the process using the process-specific intrusion detection signature to detect an intrusion; and communication means coupling the one or more machines with the security operation center." (Emphasis added.) Gluck fails to cure the defects of Trostle discussed above. Thus, for at least the reasons

discussed above in connection with claim 21, independent claim 29 should be in condition for allowance.

In addition, the Office now acknowledges that Trostle fails to teach obtaining an application-specific intrusion detection signature (see OA mailed 07/17/2006 at page 6, lines 5-6; page 9, lines 18-19; and page 13, lines 19-20) and relies on Gluck for this subject matter. Gluck describes a method and system for updating virus signature files of a computer system. (*See* Gluck at Abstract.) But Gluck never describes the virus signatures as being application-specific. Moreover, the Office never in fact asserts that Gluck describes a virus signature that is specific to an application whose network communications are being monitored using that virus signature. Thus, the rejection fails to address all the elements of independent claims 1, 12, and 29.

A prima facie case of obviousness has not been established because the proffered motivation to combine (*see* OA mailed 07/17/2006 at page 6, line 15 to page 7, line 2) is insufficient and the proposed combination would not result in the presently claimed subject matter. The proposed combination of Trostle with Gluck (the efficacy of which is not conceded) would still be completely different than the claimed obtaining an application-specific intrusion detection signature, and monitoring network communications for the invoked application

using the application-specific intrusion detection signature to detect an intrusion. As described in the Specification:

> The present inventor recognized the potential advantages of providing network intrusion detection systems and techniques that accurately identify and take into consideration the network applications currently running on a computing system/machine in a networked environment. When applications invoked on a networked machine are accurately identified, network communications for invoked applications may be monitored for application-specific intrusion signatures, and abnormal application behavior may be detected. Moreover, intrusion signatures and behavior criteria may be dynamically loaded from a remote security operation center.

(*See* Specification at ¶ 19.) Neither Trostle nor Gluck (either alone or in combination) describe monitoring network communications for an invoked application (or a process) using an application-specific intrusion detection signature (or a process-specific intrusion detection signature) to detect an intrusion.

For at least these additional reasons, independent claims 1, 12, and 29 (and dependent claim 23) should be in condition for allowance. Dependent claims 2-11, 13-20, and 30 should be patentable based on the above arguments and the additional recitations they contain. For example, with respect to claims

2, 13, and 30, the cited portion of Trostle (col. 3, lines 19-30) describes how the hash function and the trusted hash value can be downloaded during pre-boot in a manner that is transparent to the user and provides a trusted technique for detecting illicit changes to executable programs. Trostle describes detecting whether an original application has been modified by a rogue piece of software, not tracking network actions taken by the application. Trostle does not describe tracking one or more characteristics of network communications to identify process-specific abnormal communication behavior. The previously presented arguments regarding this clear distinction between Trostle and the present claims have not been addressed. Since nothing in Trostle can be even remotely considered similar to this claimed subject matter, reconsideration of the rejection of claims 2, 13, and 30 is respectfully requested.

Claim 3 recites, "wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds." The cited portion of Trostle (col. 5, lines 50-52) describes login authentication for a user. This bears no relation whatsoever to the claimed subject matter.

Thus, reconsideration of the rejection of claim 3 is respectfully requested.

Claim 4 recites, "wherein at least one of the one or more configurable thresholds comprises a threshold set by monitoring communications for the invoked application during a defined time window." The cited portion of Trostle (col. 1, line 66 to col. [2], line 3) states, "Briefly, according to the present invention, during pre-boot (i.e., the period of time prior to initiating operation of the workstation operating system), a networked workstation performs an intrusion detection hashing function on selected workstation executable program(s)." This bears no relation whatsoever to the claimed subject matter. Thus, reconsideration of the rejection of claim 4 is respectfully requested.

Claims 5 and 14 recite, "wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application." (Emphasis added.) As discussed above, Trostle describes detection operations performed before the operating system is booted, and thus cannot be considered to describe invoking a network intrusion detection system component with the invoked application, as claimed. (*See e.g.*, the Specification at ¶ 38.) Moreover, the cited portion of Trostle

(col. 1, lines 39-41) merely states, "Intrusion detection programs (i.e., virus checking programs) are commonly used in order to detect unauthorized modifications to executable programs." This clearly does not anticipate the claimed subject matter since it says nothing about when or how the intrusion detection programs are invoked. Thus, reconsideration of the rejection of claims 5 and 14 is respectfully requested.

Claims 6 and 15 recite, "wherein the network intrusion detection system component and the invoked application run within a single execution context." The Specification explicitly defines "execution context" as "a set of processing cycles given to a process, such as a task in a multitasking operating system." (*See* Specification at ¶ 17.) The cited portion of Trostle (col. 4, lines 32-35) describes a NIC (Network Interface Card) that includes a BIOS ROM (Basic Input/Output System Random Access Memory) that contains program instructions executed in the CPU (Central Processing Unit) during initialization in order to initiate downloading of executable pre-boot software modules resident on a server. This bears no relation whatsoever to the claimed subject matter. Thus, reconsideration of the rejection of claims 6 and 15 is respectfully requested.

Furthermore, for the rejections of claims 7-11, 16-20, and 22-28, the cited portions of Trostle also bear no relation whatsoever to the claimed subject matter. Thus, there are clear legal and factual deficiencies in the current rejections, and reconsideration of the rejection of claims 7-11, 16-20, and 22-28 is respectfully requested.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific issue or comment does not signify agreement with or concession of that issue or comment. Because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

It is respectfully suggested for all of these reasons, that the current rejections are overcome, that none of the cited art teaches or suggests the features which are claimed, and therefore that all of these claims should be in condition for allowance. A formal notice of allowance is thus respectfully requested.

The undersigned would like to avoid the necessity of filing an appeal. Thus, in the absence of a forthcoming notice of allowance, a telephone interview with the Examiner is respectfully requested to resolve any remaining issues.

Please apply the one month extension of time fee, plus any other necessary charges or credits, to Deposit Account No. 06-1050.

Respectfully submitted,

Date: November 17, 2006

Scott C. Harris
Reg. No. 32,030
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. **20985**
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099